REMARKS

This Amendment is submitted in response to the Office Action dated November 20, 2002, having a shortened statutory period set to expire February 20, 2003. Claim 15 is pending. Applicant has amended Claim 15. No new matter has been introduced by this amendment.

Claim Rejections - 35 U.S.C. § 103

On page two of the present Office Action, Claim 15 has been rejected under 35 U.S.C. 103(a) as being unpatentable over *Chang* (US Patent 5,848,400) in view of *Arnold* et al. (US Patent 4,558,176) and further in view of Rosen (US Patent 6,047,067) and further in view of *Merritt* (US Patent 5,475,756). That rejection is respectfully traversed and reconsideration of the claim is requested.

On page 3 of the present Office Action, it is suggested that it would have been obvious to transmit a second copy of the encrypted electronic check to the clearinghouse, since it is mere duplication of a method step. While the mere duplication itself may be obvious, Applicant points out that the motivation to perform the second step is lacking within the *Rosen* reference. Nothing within the *Rosen* reference suggests that there would be any advantage to transmitting a second copy of the electronic check. Similarly, the *Merritt* reference also referred to in the rejection on page 3, fails to suggest any advantage to transmitting a second copy of the encoded electronic check.

On page 3 of the present Office Action, it is further suggested that elements 7 and 8 of Claim 1 are disclosed by *Merritt* at column 7, lines 17-34 and Figure 4. Therein, *Merritt* teaches authentication at an ATM. The bank's host sends an encrypted PIN number for a user to an ATM along with a personal security phrase. When the user enters his PIN into the ATM, the ATM encrypts it using a one-way function and compares the result with the value received from the bank's host. If they are identical, the ATM permits the transaction to proceed.

Claim 1 has been amended to recite:

comparing said encrypted first copy of said electronic check that has been transmitted over an unsecure communication link to said encrypted second copy of said electronic check that has been transmitted over an unsecure communication link; and

responsive to determining that said encrypted first copy of said electronic check matches said encrypted second copy of said electronic check and that the payment authorization has been received, processing a transaction transferring funds from said payor's bank to said payee's bank.

Here, only the bank transmits an encrypted PIN number over an unsecure link. The user's entered PIN number is encrypted and compared directly at the ATM machine location. No transmission occurs. Consequently, the Examiner's suggestion that someone skilled in the art would be motivated at the time of the invention to combine the cited references lacks the motivation to combine the references in the way recited in Claim 15.

As has been explained above, no other reference, including *Merritt*, suggests transmitting a second copy of the encrypted check over an unsecure communication link. Even the addition of *Merritt's* teaching does not suggest this step, since *Merritt* teaches that the user will provide the encrypted key for comparison at the destination. However, this method of authentication is well known and is not what is taught by the present invention.

In the present invention, the processor, or user, at the destination where the comparison step is performed does not know the actual contents of the encrypted check. In the present invention, the method allows the processor (i.e., the clearinghouse) to perform the comparison and authentication step without having to know the content of the encrypted check. This significant advantage in financial transactions security and fraud prevention is not shown or suggested by any other references cited, nor is it suggested to one of ordinary skill in the art at the time the invention was made by reference to all of the prior art references. In the prior art, including *Merritt*, a user with knowledge of the encoded data is required to be located at the place of comparison in order to implement the authentication.

In summary, Applicants respectfully submit that the steps of

> *comparing said encrypted first copy of said electronic check that has been transmitted over an unsecure communication link to said encrypted second copy of said electronic check that has been transmitted over an unsecure communication link; and*
>
> *responsive to determining that said encrypted first copy of said electronic check matches said encrypted second copy of said electronic check and that the payment authorization has been received, processing a transaction transferring funds from said payor's bank to said payee's bank.*

are not shown or suggested by the prior art, since no reference suggests transmitting two separate copies of the encrypted electronic funds over an unsecure communication link as part of the fraud-prevention methodology of authentication. Consequently, Applicant respectfully requests reconsideration of Claim 15 and submits that the rejection of Claim 15 should be withdrawn.

No fee is believed to be required; however, in the event any additional fees are required, please charge any fee associated with an extension of time, as well as any other fee necessary to further the prosecution of this application to IBM Corporation **Deposit Account No. 09-0447.**

Respectfully submitted,

Craig Yudell

Craig J. Yudell, *Registration No. 39,083*
BRACEWELL & PATTERSON, L.L.P.
P. O. Box 969
Austin, Texas 78767-0969
(512) 472-7800
ATTORNEY FOR APPLICANTS

REDACTED CLAIMS

Please amend the claims as follows:

15. (Twice Amended) A method of processing an electronic check, comprising:

receiving an electronic check encrypted using a one-time pad at a business;

transmitting an encrypted first copy of said electronic check to a payor's bank and an encrypted second copy of said electronic check to a payee's bank;

decoding said encrypted first copy of said electronic check at said payor's bank using a copy of said one-time pad;

authenticating said electronic check;

transmitting said encrypted first copy of said electronic check over an unsecure communication link to a clearinghouse with a payment authorization;

transmitting said encrypted second copy of said electronic check over an unsecure communication link to said clearinghouse;

comparing said encrypted first copy of said electronic check that has been transmitted over an unsecure communication link to said encrypted second copy of said electronic check that has been transmitted over an unsecure communication link; and

responsive to determining that said encrypted first copy of said electronic check matches said encrypted second copy of said electronic check and that the payment authorization has been received, processing a transaction transferring funds from said payor's bank to said payee's bank.

16. (Canceled)

17. (Canceled)

18. (Not elected) A method of securing transmission of a global transponder location, comprising:

receiving a request packet via a cellular communications link to said global transponder;

encrypting a data packet containing a latitude and a longitude for a location of said global transponder using a one-time pad containing within said global transponder; and

transmitting said encrypted data packet to a central computer over said cellular communications link.

19. (Not elected) The method of claim 18, wherein said step of encrypting a data packet further comprises:

locating an identifier within said request packet;

comparing said identifier to a plurality of identifiers in said global transponder, wherein identifier within said plurality of identifiers is associated with a sheet within said one-time pad;

responsive to determining that said identifier within said request packet does not match any identifier within said plurality of identifiers, terminating said cellular communications link; and

responsive to determining that said identifier within said request packet matches an identifier within said plurality of identifiers, encrypting said data packet using a sheet within said one-time pad associated with said matching identifier.

20. (Not elected) A global transponder, comprising:

a processor connected to a memory containing a one-time pad;

a cellular modem connected to said processor and an antenna;

a GPS chip set connected to said processor and said antenna, said GPS chip set providing GPS fix data to said processor,

wherein said processor, responsive to receiving a call through said cellular modem, encrypts said GPS fix data using said one-time pad for transmission via said cellular modem.

31. (Not elected) A global transponder, comprising:

a processor connected to a memory containing a one-time pad;

a cellular modem connected to said processor and an antenna;

a GPS chip set connected to said processor and said antenna, said GPS chip set providing GPS fix data to said processor,

wherein said processor, responsive to receiving a call through said cellular modem, encrypts said GPS fix data using said one-time pad for transmission via said cellular modem.